Информационная безопасность

Методы и средства защиты информации

Получение ценной информации злоумышленником приносит ему обязательный доход и причиняет, как правило, значительный ущерб истинным владельцам этой информации. Именно поэтому появился термин «компьютерная (информационная) преступность».

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

В области компьютерных систем и информационных технологий обеспечение информационной безопасности подразумевает:

- - надежность работы компьютерных средств;
- - сохранность данных;
- - защиту информации от внесения в нее изменений неуполномоченными лицами;
- - сохранение тайны переписки в электронной связи и электронных коммуникациях.

Под безопасностью информационной системы понимается ее защищенность от случайного или преднамеренного вмешательства в ее работу, а также от попыток хищения, модификации или разрушения ее компонентов и ресурсов.

Защита информации

- это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Средства защиты информации, т.е. средства, обеспечивающие информационную безопасность, должны решать следующие три основные задачи:

- обеспечивать **конфиденциальность** информации;
- обеспечивать **целостность** информации;
- обеспечивать **доступность** информации.

Конфиденциальностью информации называется ее защищенность от несанкционированного ознакомления

- Для служебного пользования
- Секретно
- Совершенно секретно
- Особой важности

Целостностью информации называется ее защищенность от несанкционированного изменения и разрушения.

Доступность информации – это возможность ее получения допущенным (легальным) пользователем за приемлемое время при любых мерах и системах ее защиты.

Обеспечение информационной безопасности – это совокупность правовых, организационных и программно-технических методов и средств защиты информационных ресурсов, позволяющих проводить принятую политику информационной безопасности.

Правовое обеспечение информационной безопасности

- призвано поддерживать в обществе негативное отношение к нарушителям информационной безопасности, сформировать карательные меры воздействия на злостных нарушителей.

Организационное обеспечение информационной безопасности

- имеет своей задачей формирование и проведение политики информационной безопасности на предприятиях, в организациях, учреждениях и т.д. Сюда относится обучение персонала, организация охраны компьютеров и внутренних линий связи и т.д.

Программно-техническое обеспечение информационной безопасности

- призвано осуществлять конкретные меры безопасности на уровне компьютерных систем и сетей.

К средствам программно-технического обеспечения информационной безопасности относятся, например, следующие:

- - межсетевые экраны (брандмауэры) – программно-технические средства, препятствующие несанкционированному перемещению данных между сетями,
- - программы идентификации (опознания) и аутентификации (установления подлинности) пользователей и адресантов,
- - программы протоколирования и аудита систем и сетей (аудит – это регистрация основных действий для последующего анализа),
- - программы антивирусной защиты информации (компьютерный вирус – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных, и предназначенный для выполнения несанкционированных действий на компьютере),
- - программы стеганографической защиты сообщений (т.е. маскирование закрытой информации среди открытых данных),
- - программы криптографической защиты сообщений, в которых реализуются методы и способы преобразования (шифрования) информации с целью скрыть ее истинное содержание от лиц, не имеющих полномочий знать эту информацию,
- и др.

Спасибо за внимание!